

Crittografia e Protocolli di Sicurezza

Ing. Emilio Spinicci

07/04/2004

1

Argomenti della lezione

- ◆ Introduzione
- ◆ Principi di Crittografia
- ◆ Protocolli di Sicurezza
- ◆ Attacchi ai Protocolli di Sicurezza

07/04/2004

2

Introduzione

La crittografia è una disciplina che si applica principalmente nelle operazioni di comunicazione in presenza di avversari.

07/04/2004

3

Introduzione

Una comunicazione è un'operazione in cui due soggetti legittimi (*mittente* e *destinatario*) articolano uno scambio di pacchetti informativi su di un qualche mezzo trasmissivo (canale), ed è potenzialmente soggetta alle azioni di una terza parte illegittima (avversario o *intruso*).

07/04/2004

4

Introduzione

Obiettivo

Consentire a due soggetti di comunicare su un canale di comunicazione potenzialmente insicuro, affinché un eventuale avversario non possa comprendere il contenuto informativo dei messaggi scambiati. Questo obiettivo può essere perseguito utilizzando *algoritmi crittografici*.

07/04/2004

5

Introduzione

Principali requisiti di un sistema crittografico

- ◆ *Segretezza* delle comunicazioni;
- ◆ *Autenticazione* delle parti;
 - paternità del messaggio;
 - schema di firma;
- ◆ *Integrità*;
- ◆ *Non-ripudiabilità*;

07/04/2004

6

Principi di Crittografia - definizioni

- ◆ *Sistema crittografico*
sistema che realizza funzionalità di natura crittografica: funzionalmente, può essere un *algoritmo* o un *protocollo*.

07/04/2004

7

Principi di Crittografia - definizioni

- ◆ **Testo in chiaro** (*plaintext*)
Contenuto originale del messaggio, *intelligibile* a chiunque;
- ◆ **Testo cifrato** (*cyphertext*)
Alterazione volontaria e reversibile del contenuto informativo del messaggio originale, compiuta allo scopo di rendere lo stesso *non intelligibile*;

07/04/2004

8

Principi di Crittografia - definizioni

◆ Chiave

Una chiave K è una sequenza di bit di lunghezza finita, generata in modo casuale e imprevedibile tramite una *sorgente di casualità effettiva*, impiegata come ingresso di un algoritmo crittografico avente un'uscita dipendente da essa.

07/04/2004

9

Principi di Crittografia - definizioni

In relazione alle proprietà di sicurezza previste dal sistema crittografico, si hanno le seguenti tipologie di chiavi:

◆ Chiave privata (segreta)

una chiave K_s è segreta se è conosciuta solo dall'utente proprietario;

◆ Chiave condivisa

una chiave K_{ab} è condivisa se è conosciuta solo dalla coppia di utenti A e B accreditati come possessori;

◆ Chiave pubblica

una chiave K_p è pubblica se deve essere conosciuta da tutti gli utenti che ne devono fare uso.

07/04/2004

10

Principi di Crittografia - definizioni

Algoritmi crittografici

Un **algoritmo di cifratura** E è un algoritmo che, ricevuti in ingresso un messaggio in chiaro M e una **chiave di cifratura** K_e , produce in uscita un messaggio cifrato C : $C = E_{K_e}(M)$

Un **algoritmo di decifratura** D è un algoritmo che, ricevuti in ingresso un messaggio cifrato C e la corrispondente **chiave di decifratura** K_d , restituisce il messaggio in chiaro M : $M = D_{K_d}(C)$

07/04/2004

11

Principi di Crittografia - definizioni

Algoritmi crittografici

Un **algoritmo crittografico** A è un sistema costituito da un algoritmo di cifratura E e dal corrispondente algoritmo di decifratura D , e che si avvale quindi delle rispettive chiavi di cifratura K_e e di decifratura K_d .

07/04/2004

12

Proprietà degli algoritmi crittografici

- ◆ *Assunzione della Cifratura Perfetta*

Si può ottenere il contenuto in chiaro di un messaggio solo disponendo dell'apposita chiave di decifratura

($P(x=x^*)=P(x=x^*|y=y^*)$, x in chiaro e y cifrato \rightarrow inviolabilità computazionale dell'algoritmo crittografico).

- ◆ *Assunzione di Kerchhoff*

La sicurezza di un algoritmo crittografico non deve dipendere dalla sua segretezza \rightarrow la conoscenza di un algoritmo (ricavabile tramite analisi hardware o software) non deve compromettere le funzionalità da esso previste.

07/04/2004

13

Principi di Crittografia - definizioni

Algoritmo a chiave segreta (simmetrico)

Un algoritmo crittografico A si dice *a chiave segreta (simmetrico)* se:

- l'algoritmo di cifratura E e quello di decifratura D coincidono o sono strutturalmente simili;
- le chiavi K_e e K_d coincidono o sono ricavabili l'una dall'altra: $K = K_e \cong K_d$;
- la chiave K è una chiave segreta.
- esempio: algoritmo *DES*.

07/04/2004

14

Principi di Crittografia - definizioni

Proprietà degli algoritmi simmetrici

$$(P_1) \quad \forall M \in M^*, \forall K \in K^* : D_K(E_K(M)) = M;$$

$$(P_2) \quad \forall M \in M^*, \forall K \in K^* : E_K(D_K(M)) = M;$$

07/04/2004

15

Principi di Crittografia - definizioni

Algoritmo a chiave pubblica

Un algoritmo crittografico A si dice *a chiave pubblica* se:

- le chiavi K_e e K_d sono diverse: $K_e \neq K_d$; inoltre, la chiave K_e è pubblica, mentre K_d è una chiave privata: $K_e \approx K_p, K_d \approx K_s$.
- generalmente, l'algoritmo di cifratura E e quello di decifratura D sono strutturalmente diversi.
- esempio: algoritmo *RSA*.

07/04/2004

16

Principi di Crittografia - definizioni

Proprietà degli algoritmi a chiave pubblica

$$(P_3) \quad \forall M \in M^*, \forall K_p, K_s \in K^* : \\ D_{K_s}(E_{K_p}(M)) = M;$$

$$(P_4) \quad \forall M \in M^*, \forall K_p, K_s \in K^* : \\ E_{K_p}(D_{K_s}(M)) = M;$$

07/04/2004

17

Principi di Crittografia - definizioni

Proprietà degli algoritmi a chiave pubblica

Se l'algoritmo a chiave pubblica è simmetrico

$$(D_K \cong E_K):$$

$$(P_5) \quad \forall M \in M^*, \forall K_p, K_s \in K^* : \\ D_{K_p}(E_{K_s}(M)) = M;$$

$$(P_6) \quad \forall M \in M^*, \forall K_p, K_s \in K^* : \\ E_{K_s}(D_{K_p}(M)) = M;$$

07/04/2004

18

Principi di Crittografia - definizioni

Convenzioni dell'ingegneria dei protocolli

$$E_K(\dots) \cong \{\}_K$$
$$D_K(\dots) \cong \{\}_K$$
$$K_p \cong K, K_s \cong K^{-1}$$

$$(P_6) \{\{\ M\}_K\}_K = M;$$

(alg. A chiave segreta)

$$(P_7) \{\{\ M\}_{K^{-1}}\}_K = M,$$
$$\{\{\ M\}_K\}_{K^{-1}} = M;$$

(alg. A chiave pubblica, simmetrici);

07/04/2004

19

Principi di Crittografia - algoritmi

Utilizzo degli algoritmi a chiave segreta

Due utenti che vogliono avvalersi di un algoritmo a chiave segreta devono condividere in esclusiva una chiave segreta K_{ab} .

Il messaggio trasmesso viene prima cifrato e poi decifrato con la stessa chiave K_{ab} :

$$\{\{\ M\}_{K_{ab}}\}_{K_{ab}} = M$$

07/04/2004

20

Principi di Crittografia - algoritmi

Vantaggi degli algoritmi a chiave segreta

- Segretezza del messaggio (autenticazione del destinatario);
- Autenticazione del mittente;

(...in quanto solo mittente e destinatario sono proprietari della chiave dell'algoritmo, e quindi solo essi possono cifrare e decifrare un testo...)

- Integrità del messaggio;

(...in caso di alterazione del contenuto, il messaggio decifrato risulterà privo di senso...)

07/04/2004

21

Principi di Crittografia - algoritmi

Svantaggi degli algoritmi a chiave segreta

Le proprietà precedenti valgono nell'ipotesi che un eventuale intruso non sia in grado di ottenere la chiave segreta; poiché per ipotesi il canale di comunicazione è non sicuro, le parti non possono affidarsi ad esso per scambiarsi la chiave di sessione.

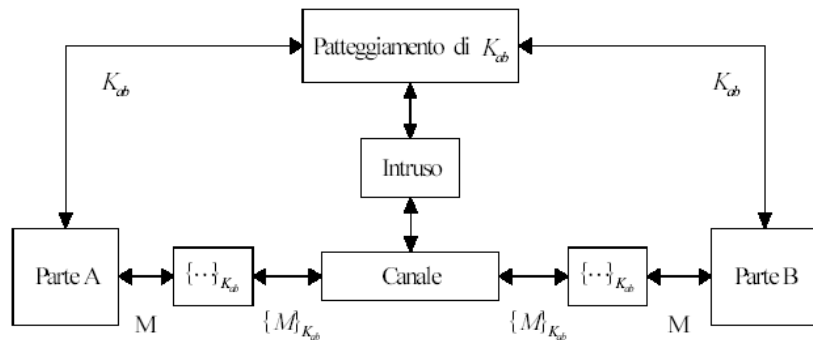
Occorre quindi un canale sicuro (linea dedicata) senza possibilità di accessi esterni.

→ Soluzione costosa e non praticabile su larga scala.

07/04/2004

22

Comunicazione privata tramite algoritmo a chiave segreta



Principi di Crittografia - algoritmi

Utilizzo degli algoritmi a chiave pubblica

In una comunicazione tramite algoritmo a chiave pubblica, a ciascuna delle parti è associata una coppia di chiavi:

$$\langle K_a, K_a^{-1} \rangle, \langle K_b, K_b^{-1} \rangle$$

La chiave K è pubblica ed accessibile a tutti gli utenti, mentre la chiave K^{-1} è privata e di proprietà di un unico utente

07/04/2004

24

Principi di Crittografia - algoritmi

Invio di un messaggio A → B

Il mittente A di un messaggio M_a si avvale della chiave pubblica K_b del destinatario B per cifrare il messaggio in chiaro; il messaggio cifrato $C_a = \{M_a\}_{K_b}$ è così inviato al destinatario B.

07/04/2004

25

Principi di Crittografia - algoritmi

Invio di un messaggio A → B

Il destinatario B recupera il testo in chiaro:

$$M_a = \{C_a\}_{K_b^{-1}} = \{\{M_a\}_{K_b}\}_{K_b^{-1}}$$

...analogamente nel caso B → A.

07/04/2004

26

Principi di Crittografia - algoritmi

Vantaggi degli algoritmi a chiave pubblica

- Segretezza del messaggio (autenticazione del destinatario);
- Integrità del messaggio;

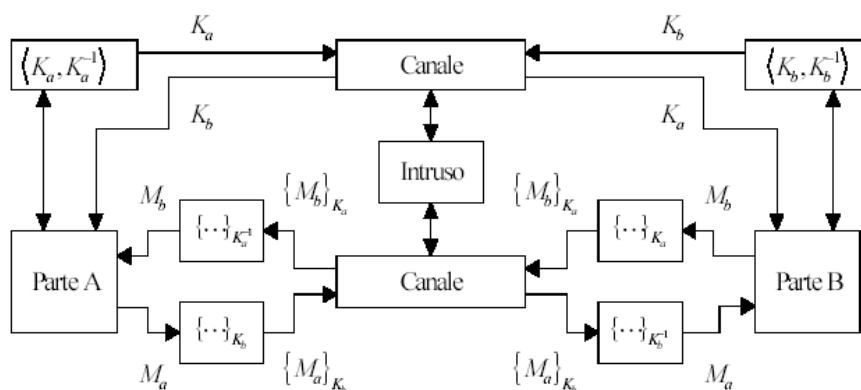
Svantaggi degli algoritmi a chiave pubblica

- Autenticazione del mittente non garantita: poiché la chiave pubblica è a disposizione di chiunque, in uno scambio $A \rightarrow B$ un eventuale intruso può cifrare un messaggio con chiave K_b ed impersonare A al cospetto di B.

07/04/2004

27

Comunicazione privata tramite algoritmo a chiave pubblica



07/04/2004

28

Principi di Crittografia - algoritmi

Autenticazione del mittente tramite cifratura doppia

Si può allora pensare di utilizzare, in uno scambio $A \rightarrow B$, una doppia cifratura del messaggio, prima con la chiave privata di A, poi con quella pubblica di B:

$$C_a = \{\{M_a\}_{K_a^{-1}}\}_{K_b}$$

In ricezione, B decifrerà il messaggio con la propria chiave privata K_b^{-1} , ottenendo

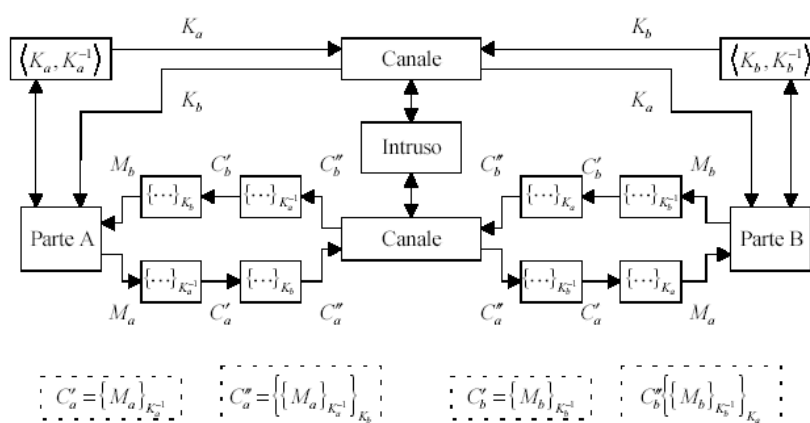
$$\{M_a\}_{K_a^{-1}}$$

poi con la chiave pubblica di A per riottenere il messaggio originale $\{\{M_a\}_{K_a^{-1}}\}_{K_a} = M_a$

07/04/2004

29

Comunicazione privata tramite algoritmo a chiave pubblica con autenticazione



07/04/2004

30

Principi di Crittografia - algoritmi

Autenticazione del mittente tramite cifratura doppia

La cifratura più interna con la chiave privata del mittente A costituisce una sorta di firma

(K_a^{-1} è nota solo ad A).

Tale firma è protetta dalla cifratura più esterna con la chiave pubblica del ricevente B, in modo che solo quest'ultimo potrà aprire il messaggio e rimuoverla (la firma è una cifratura) per comprendere il suo contenuto.

07/04/2004

31

Principi di Crittografia - algoritmi

Verifica dell'integrità del messaggio tramite Digest

La doppia cifratura garantisce inoltre l'integrità del messaggio ma è computazionalmente costosa;

→ Generazione del *Digest* (riassunto) ottenuto dal messaggio mediante una *funzione Hash crittografica* (resistente alle collisioni).

→ Il Digest è trasmesso assieme al messaggio: il destinatario verificherà che il digest $D=H(M)$ ricevuto corrisponda a quello da lui calcolato sul testo in chiaro, tramite $H()$, stabilendo così l'integrità del messaggio ricevuto.

07/04/2004

32

Protocolli di sicurezza - definizioni

◆ *Protocollo di sicurezza*

Un protocollo di sicurezza è una sequenza di azioni (passi) che coinvolge due o più parti, denominate *principali*, finalizzata all'instaurazione di una comunicazione sicura fra di esse, al riparo dalle azioni di un possibile intruso.

L'insieme dei passi specificati costituisce la *sessione* del protocollo.

07/04/2004

33

Protocolli di sicurezza - definizioni

Classificazione dei protocolli di sicurezza

In base all'algoritmo crittografico scelto:

- ◆ Protocolli a chiave segreta;
- ◆ Protocolli a chiave pubblica;

In base allo scopo finale:

- ◆ Protocolli di autenticazione e scambio chiavi (es: protocollo **I**nternet **K**ey **E**xchange);
- ◆ Protocolli per la gestione di transazioni (e-commerce, protocollo **S**ecure **E**lectronic **T**ransaction);

... si parlerà quindi ad esempio di protocollo di autenticazione a chiave pubblica...

07/04/2004

34

Protocolli di sicurezza - definizioni

Parte fiduciaria

- ◆ I protocolli *a tre parti* prevedono l'intervento, oltre che dei due principali, di una terza parte detta *parte fiduciaria*, che ha il compito di contribuire al conseguimento dell'autenticazione tra le parti, provvedendo alla generazione delle chiavi di sessione ed alla distribuzione delle chiavi pubbliche. La parte fiduciaria opera quindi una sorta di *certificazione delle parti*.

07/04/2004

35

Protocolli di sicurezza

Il contesto dell'autenticazione

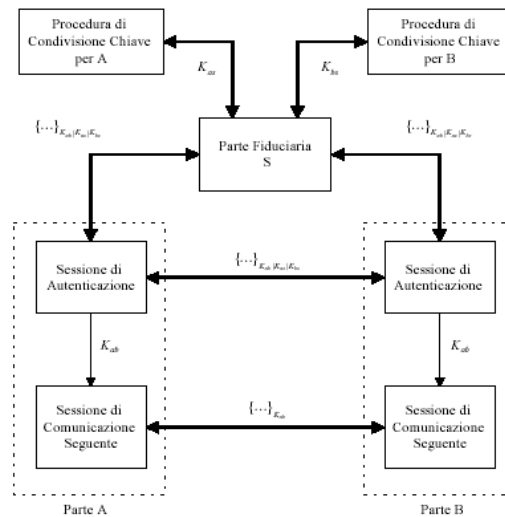
E' prevista una *sessione di autenticazione* in cui, tramite la parte fiduciaria S , le parti A e B si identificano reciprocamente, prima dello scambio di messaggi nella *sessione di comunicazione*.

Nello schema di *Diffie-Hellman*, A e B pattuiscono con S rispettivamente le chiavi segrete K_{as} e K_{bs} . Attraverso la comunicazione privata con S , A e B si identificano e pattuiscono la chiave segreta K_{ab} per la successiva comunicazione.

07/04/2004

36

Schema di Diffie-Hellman a chiave segreta



07/04/2004

37

Protocolli di sicurezza

Struttura di un protocollo di sicurezza

Un generico *atto comunicativo* tra i principali X e Y in cui X invia il messaggio M a Y , relativo al passo n , si rappresenta in simboli come segue:

$$(n) X \rightarrow Y : M$$

Ogni *messaggio* M è costituito da una lista di componenti elementari, dette *words*, o da composizioni di quest'ultime. Le *words* sono caratterizzate da un *tipo*, che ne individua la funzione all'interno del protocollo:

$$word_1, word_2, \dots, word_n$$

07/04/2004

38

Protocolli di sicurezza

Struttura di un protocollo di sicurezza

Ogni *word* può essere trasmessa in chiaro o cifrata secondo quanto stabilito dal protocollo; un generico messaggio avrà quindi la forma :

$$\{word_1, \{word_2\}_{K_1} \dots, word_n\}$$

È possibile anche una struttura nidificata, con operatori di cifratura annidati, come nel seguente esempio:

$$\{word_1, \{word_2\}_{K_1}, \{\{word_3\}_{K_2} \{word_4\}\}, \{word_5, word_6\}_{K_1}, \dots, word_n\}_{K_3}$$

07/04/2004

39

Protocolli di sicurezza

Principali tipologie di words

- ◆ *identificatori di principali;*
- ◆ *chiavi, segrete, private, pubbliche o di sessione;*
- ◆ *identificatori di freschezza:*
 - *nonce* (contrazione di *only-once*): componente numerica casuale e imprevedibile, *inedita* in ogni precedente sessione del protocollo, generata per smascherare eventuali repliche, da parte di un intruso, di messaggi intercettati in sessioni precedenti del protocollo.
 - *marca temporale* (ottenuta tramite un clock);
 - *contatori;*

07/04/2004

40

Protocolli di sicurezza

Utilizzo dei Nonces – Messaggi di sfida

$$(n') A \rightarrow B : \dots, N, \dots$$
$$(n'') B \rightarrow A : \dots, \{N\}_K, \dots$$

- ◆ Nel passo (n') A invia a B un messaggio contenente al suo interno anche il nonce N ;
- ◆ Al passo (n'') B deve rispondere con un messaggio che prevede la presenza del nonce N cifrato con una chiave K , nota ad A e B ;

07/04/2004

41

Protocolli di sicurezza

Utilizzo dei Nonces – Messaggi di sfida

$$(n') A \rightarrow B : \dots, N, \dots$$
$$(n'') B \rightarrow A : \dots, \{N\}_K, \dots$$

A decifra il nonce cifrato con K e, se verifica che quanto ottenuto coincide con il nonce inviato nel primo messaggio, A può essere sicuro che il messaggio in (n'') è stato inviato dopo il messaggio al passo (n') (non si tratta di un messaggio replicato).

In questo modo viene garantita la recente generazione del messaggio, dato che in esso è presente un'informazione funzionalmente dipendente da quella del messaggio che lo ha preceduto nella stessa esecuzione.

07/04/2004

42

Attacchi ai protocolli di sicurezza

Tattiche dell'intruso

- ◆ *Attacco passivo*: attacco in cui l'intruso si limita ad intercettare e memorizzare i messaggi scambiati nell'esecuzione di un protocollo, per ottenere la maggiore quantità possibile di informazioni sulle parti, senza impedire che i messaggi intercettati raggiungano integri i destinatari designati.

L'intruso potrà impiegare tali informazioni per sottoporre i testi cifrati a procedimenti crittoanalitici (analisi *cyphertext-only*, *known plaintext*, ...) da cui dedurre le chiavi di sessioni e/o i messaggi in chiaro corrispondenti a quelli cifrati.

07/04/2004

43

Attacchi ai protocolli di sicurezza

Tattiche dell'intruso

- ◆ *Attacco attivo*: l'intruso interagisce attivamente con la rete di comunicazione e con le parti del protocollo, alterando il normale svolgimento delle esecuzioni del protocollo.

07/04/2004

44

Attacchi ai protocolli di sicurezza

Principali interazioni dell'intruso in un attacco attivo

- ◆ Introduzione nell'esecuzione del protocollo di messaggi generati dall'intruso per aprire sessioni di autenticazione con qualsiasi utente;
- ◆ Invio di messaggi per conto di un altro utente;
- ◆ Alterazione o soppressione di messaggi destinati a un determinato principale (*Denial of Service*);
- ◆ Replica in una sessione del protocollo di messaggi memorizzati in sessioni concluse in precedenza;

07/04/2004

45

Attacchi ai protocolli di sicurezza

Convenzioni relative agli attacchi

- ◆ $I, A \rightarrow B : msg$
A invia il messaggio *msg* al principale *B*, oppure l'intruso *I* lo invia per conto di *A*, impersonandolo a sua insaputa al cospetto di *B* (*attacco eseguito generalmente all'inizio del protocollo*).
- ◆ $A \rightarrow I, B : msg$
I intercetta e memorizza un messaggio inviato da *A* a *B*, lasciandolo però giungere inalterato al destinatario designato *B*.
(*l'intruso riutilizzerà il messaggio intercettato nella successiva esecuzione del protocollo*).

07/04/2004

46

Attacchi ai protocolli di sicurezza

Convenzioni relative agli attacchi

- ◆ $I(A) \rightarrow B: msg$
L'intruso I appare A al cospetto di B . E' il tipo di azione più frequente che un intruso compie negli attacchi. In genere, il messaggio inviato è stato catturato da un atto comunicativo avvenuto in precedenza.
- ◆ $A \rightarrow I(B): msg$
L'intruso I intercetta e memorizza un messaggio inviato da A al ricevente designato B , rimuovendo il messaggio stesso dal canale di comunicazione. Si tratta dell'azione più intrusiva a danno di un atto comunicativo.

07/04/2004

47

Attacchi ai protocolli di sicurezza

Convenzioni relative agli attacchi

- ◆ $I \rightarrow B: msg$
L'intruso I invia un messaggio a B interpretando esplicitamente se stesso. Si tratta di un'azione possibile quando l'intruso è un principale, in grado di interagire con le altre parti senza destare sospetti.
- ◆ $A \rightarrow I: msg$
L'intruso I riceve da A un messaggio a lui espressamente rivolto. Anche in questo caso, l'intruso è una parte accreditata del sistema.

07/04/2004

48

Attacchi ai protocolli di sicurezza

Protocollo di Needham-Schroeder

Protocollo (versione semplificata)	Attacco al protocollo
1. $A \rightarrow B: \{N_A, M_A\}_{K_B}$	1. $A \rightarrow I: \{N_A, M_A\}_{K_I}$
2. $B \rightarrow A: \{N_A, N_B\}_{K_A}$	1'. $I(A) \rightarrow B: \{N_A, M_A\}_{K_B}$
3. $A \rightarrow B: \{N_B\}_{K_B}$	2. $B \rightarrow A: \{N_A, N_B\}_{K_A}$
	3. $A \rightarrow I: \{N_B\}_{K_I}$
	3'. $I(A) \rightarrow B: \{N_B\}_{K_B}$

07/04/2004

49

Verifica dei protocolli di sicurezza

- ◆ I passi dell'attacco al protocollo di Needham-Schroeder sono stati individuati mediante verifica algoritmica del protocollo tramite *Model-Checking*.
- ◆ *Le critiche rivolte al protocollo di Needham-Schroeder ne hanno determinato l'evoluzione in Kerberos (Eudora).*

07/04/2004

50

Riferimenti

- ◆ G. Antini,
Introduzione alla Crittografia – sistemi crittografici simmetrici e asimmetrici.
<http://dsi.dsi.unifi.it/~fantechi/INFIND/Crittografia.pdf>
- ◆ G. Vannuccini,
La sicurezza sulla rete.
<http://best.det.unifi.it/telematica/seminari.htm>